Mutual authenticated quantum no-key encryption scheme over private quantum channel

Li Yang[1,2*], Chenmiao Wu [1,2,3]

1.State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

2.Data Assurance and Communication Security Research Center,Chinese Academy of Sciences, Beijing 100093, China

3.University of Chinese Academy of Sciences, Beijing, 100049, China

Abstract

We realize shamir's no-key protocol via quantum computation of Boolean permutation and private quantum channel. The quantum no-key (QNK) protocol presented here is one with mutual authentications, and proved to be unconditionally secure. An important property of this protocol is that0 its authentication key can be reused permanently.

Keywords:
quantum cryptography, quantum no-key encryption

1. Introduction

No-key protocol was first proposed by Shamir [1] which can be used to transmit classical messages secretly in public channel without public key or secret key. Shamir's protocol is based on discrete logarithm problem which cannot resist a man-in-the-middle (MIM) attack. The quantum version of no-key protocol based on single-photon rotations was developed in [2, 3]. The security of quantum no-key (QNK) protocol is based on the laws of quantum mechanics, rather than computational hypothesis. Other similar protocols were proposed [4–6]. A protocol proposed in [7] with inherent identification is based on quantum computing of Boolean functions which can prevent MIM attack. Ref. [8] proposed a practical quantum no-key protocol

[*] Corresponding author email: yangli@iie.ac.cn

with mutual identification, and present a newly attack named unbalance-of-information-source (UIS) attack. A 9-round QNK protocol with data origin authentication which achieves perfect security was constructed in [9]. Ref. [10, 11] are quantum message oriented protocols which is the development of Shannon's one-time-pad encryption scheme in classical cryptography. Ref. [12] presents some development of those quantum one-time pad schemes. In this paper, we propose a QNK protocol based on the algorithm presented in [10, 11]

2. Quantum no-key scheme with interactive identification

2.1. Private quantum channel

Ambainis et al. [11] defined PQC with an ancillary quantum state. Suppose $U_k, k = 1, 2, \cdots, N$ is a set of operations. Each element U_k is a $2^n \times 2^n$ unitary matrix. Let the plaintext state be a n-qubit quantum message ρ. In the encryption stage, U_k is applied to the quantum state, where k is a secret key. p_k represents the probability of choosing k as secret key.

$$\rho_c = U_k \rho U_k^\dagger. \tag{1}$$

To decrypt ciphertext, $U_k^\dagger$ is applied to ρ_c,

$$\rho = U_k^\dagger \rho_c U_k. \tag{2}$$

Quantum perfect encryption is defined in [11]: for every input state ρ, the output state is an ultimately mixed state, that is

$$\sum_k p_k U_k \rho U_k^\dagger = \frac{I}{2^n}. \tag{3}$$

[11] constructs one perfect encryption by choosing $p_k = \frac{1}{2^{2n}}$, $U_k = X^\alpha Z^\beta(\alpha, \beta \in \{0,1\}^n)$. Boykin and Roychowdhury prove that their construction is perfect.

2.2. Scheme description

Alice and Bob preshare bit strings s and r, $s \in \{0,1\}^n$, $r \in \{0,1\}^{\frac{n}{2}}$. Alice intends to transmit classical message x to Bob through quantum channel.

1. Alice randomly selects $\alpha_A, \beta_A \in \{0,1\}^n$ to encrypt $|x\rangle_I\langle x|$ with $Y^{\alpha_A}H^{\beta_A}$:

$$Y^{\alpha_A}H^{\beta_A}|x\rangle_I\langle x|H^{\beta_A}Y^{\alpha_A} = \sum_m \alpha_m|m\rangle_I\langle m|, \tag{4}$$

   The first register represents the encrytpion of plaintext.

   Then Alice does unitary transform U_s on the quantum state:

$$\begin{aligned} & U_s\big(\sum_m \alpha_m|m\rangle_I\langle m| \otimes |0\rangle_{II}\langle 0|\big)U_s^\dagger \\ = & \sum_m \alpha_m|m\rangle_I\langle m| \otimes |F_s(m)\rangle_{II}\langle F_s(m)|, \end{aligned} \tag{5}$$

   and uses r and a randomly selected bit string $r_A \in \{0,1\}^{\frac{n}{2}}$ to do exclusive-or operation to get:

$$\sum_m \alpha_m|m\rangle_I\langle m| \otimes |F_s(m) \oplus r\|r_A\rangle_{II}\langle F_s(m) \oplus r\|r_A|. \tag{6}$$

   The second register consists of the identity information about Alice.

   Finally Alice sends Bob registers I, II.

2. Bob uses preshared s to do the computation:

$$\begin{aligned} & U_s^{-1}(\sum_m \alpha_m|m\rangle_I\langle m| \otimes |F_s(m) \oplus r\|r_A\rangle_{II}\langle F_s(m) \oplus r\|r_A|)(U_s^{-1})^\dagger \\ = & \sum_m \alpha_m|m\rangle_I\langle m| \otimes |F_s(m) \oplus F_s(m) \oplus r\|r_A\rangle_{II}\langle F_s(m) \oplus F_s(m) \oplus r\|r_A| \\ = & \sum_m \alpha_m|m\rangle_I\langle m| \otimes |r\|r_A\rangle_{II}\langle r\|r_A|, \end{aligned} \tag{7}$$

   then Bob measures the second register to get the string $r\|r_A$, if the first $\frac{n}{2}$ bits are identical with r, he accepts that the message comes from Alice; otherwise, he aborts the scheme.

   Through verification, Bob randomly selects $\alpha_B, \beta_B \in \{0,1\}^n$, and uses $Y^{\alpha_B}H^{\beta_B}$ to encrypt:

$$Y^{\alpha_B}H^{\beta_B}(\sum_m \alpha_m|m\rangle_I\langle m|)H^{\beta_B}Y^{\alpha_B} = \sum_m \alpha_m^{'}|m\rangle_I\langle m|. \tag{8}$$

The first register contains the transmitted plaintext, and Bob will uses the third register to add his identity information.

Bob does transform U_s:

$$\begin{aligned} & U_s(\sum_m \alpha_m^{'}|m\rangle_I\langle m| \otimes |0\rangle_{III}\langle 0|)U_s^{\dagger} \\ = & \sum_m \alpha_m^{'}|m\rangle_I\langle m| \otimes |F_s(m)\rangle_{III}\langle F_s(m)|, \end{aligned} \qquad (9)$$

and uses r_A and a randomly selected r_B to do exclusive-or operation, the quantum state becomes:

$$\sum_m \alpha_m^{'}|m\rangle_I\langle m| \otimes |F_s(m) \oplus r_A\|r_B\rangle_{III}\langle F_s(m) \oplus r_A\|r_B|. \qquad (10)$$

then sends Alice registers I, III.

3. Alice uses s to disentangle the registers:

$$\begin{aligned} & U_s^{-1}(\sum_m \alpha_m^{'}|m\rangle_I\langle m| \otimes |F_s(m) \oplus r_A\|r_B\rangle_{III}\langle F_s(m) \oplus r_A\|r_B|)(U_s^{-1})^{\dagger} \\ = & \sum_m \alpha_m^{'}|m\rangle_I\langle m| \otimes |r_A\|r_B\rangle_{III}\langle r_A\|r_B|. \end{aligned} \qquad (11)$$

Afterwards Alice measures the third register, if first part of the result of measurement is equal to r_A, she accepts the legality of Bob; otherwise, the scheme is aborted.

Through verification, Alice decrypts with $H^{\beta_A}Y^{\alpha_A}$:

$$H^{\beta_A}Y^{\alpha_A}(\sum_m \alpha_m^{'}|m\rangle_I\langle m|)Y^{\alpha_A}H^{\beta_A} = \sum_m \alpha_m^{''}|m\rangle_I\langle m|, \qquad (12)$$

and uses s to do transform U_s as well as r, r_B to do exclusive-or operation:

$$\begin{aligned} & \sum_m \alpha_m^{''}|m\rangle_I\langle m| \otimes |0\rangle_{IV}\langle 0| \\ \rightarrow & \sum_m \alpha_m^{''}|m\rangle_I\langle m| \otimes |F_s(m) \oplus r_B\|r_C\rangle_{IV}\langle F_s(m) \oplus r_B\|r_C|, \end{aligned} \qquad (13)$$

then sends Bob registers I, IV.

4. Bob uses s to do U_s^{-1} transform to disentangle the registers:

$$\begin{aligned} & U_s^{-1}(\sum_m \alpha_m^{''}|m\rangle_I\langle m| \otimes |F_s(m) \oplus r_B\|r_C\rangle_{IV}\langle F_s(m) \oplus r_B\|r_C|)(U_s^{-1})^{\dagger} \\ = & \sum_m \alpha_m^{''}|m\rangle_I\langle m| \otimes |r_B\|r_C\rangle_{IV}\langle r_B\|r_C|. \end{aligned} \quad (14)$$

By measuring register IV, Bob can verify the legitimacy of Alice. He retains r_C to replace r. So the preshared bit strings between Alice and Bob for the next session are s and r_C.

If Bob makes sure that the message sender is Alice, he decrypts with $H^{\beta_B}Y^{\alpha_B}$:

$$H^{\beta_B}Y^{\alpha_B}(\sum_m \alpha_m^{''}|m\rangle_I\langle m|)Y^{\alpha_B}H^{\beta_B} = |x\rangle_I\langle x|, \quad (15)$$

finally Bob gets the transmitted message x.

3. Security analysis

In the first round communication, if the adversary intercept the transmitted message in the quantum channel, the message state for him is:

$$\sigma_1 = \sum_{m,s,r,r_A} \alpha_m|m\rangle_I\langle m| \otimes |F_s(m) \oplus r\|r_A\rangle_{II}\langle F_s(m) \oplus r\|r_A|. \quad (16)$$

For every given input m, $F_s(m)$ iterates through all the possible value. So the quantum state $\sum\limits_{s,r,r_A} |F_s(m) \oplus r\|r_A\rangle_{II}\langle F_s(m) \oplus r\|r_A|$ is an ultimately mixed state which has nothing to do with the value of m. Part of the ciphertext state: $\sum\limits_m \alpha_m|m\rangle_I\langle m|$ is obtained by performing H and Y on the plaintext state. Now, we firstly prove that the following proposition.

Proposition 1. *$\{p_k = \frac{1}{2^{2n}}, U_k = U_1^{\alpha}U_2^{\beta}, k = (\alpha, \beta), \alpha, \beta \in \{0,1\}^n\}$ is a quantum perfect encryption.*

Proof: Since $\{U_1^{\alpha}U_2^{\beta}, \alpha, \beta \in \{0,1\}^n\}$ is a complete orthonormal basis, any n-qubit state ρ can be represented as a linear combination of these 2^{2n} unitary matrixes:

$$\rho = \sum_{\alpha,\beta} a_{\alpha,\beta}U_1^{\alpha}U_2^{\beta},$$

where $a_{\alpha,\beta} = tr(\rho U_2^\beta U_1^\alpha)/2^n$.

Thus,

$$\begin{aligned}\sum_k p_k U_k \rho U_k^\dagger &= \frac{1}{2^{2n}} \sum_{\gamma,\delta} U_1^\gamma U_2^\delta \rho U_2^\delta U_1^\gamma \\ &= \frac{1}{2^{2n}} \sum_{\alpha,\beta} a_{\alpha,\beta} \sum_{\gamma,\delta} U_1^\gamma U_2^\delta U_1^\alpha U_2^\beta U_2^\delta U_1^\gamma.\end{aligned}$$

From $U_1U_2 = -U_2U_1$,we have $U_2^\delta U_1^\alpha = (-1)^{\alpha\cdot\delta} U_1^\alpha U_2^\delta$. Thus, the above formula can be expressed as:

$$\begin{aligned}&\frac{1}{2^{2n}} \sum_{\alpha,\beta} a_{\alpha,\beta} \sum_{\gamma,\delta} (-1)^{\alpha\cdot\delta} U_1^\alpha U_1^\gamma U_2^\delta (-1)^{\beta\cdot\gamma} U_2^\delta U_1^\gamma U_2^\beta \\ = &\frac{1}{2^{2n}} \sum_{\alpha,\beta} a_{\alpha,\beta} \sum_{\gamma,\delta} (-1)^{\alpha\cdot\delta} (-1)^{\beta\cdot\gamma} U_1^\alpha U_2^\beta.\end{aligned}$$

Because $\frac{1}{2^n}\sum_{\gamma\in\{0,1\}^n}(-1)^{\beta\cdot\gamma} = \delta_{\beta,0}$, the above formula is equal to:

$$\sum_{\alpha,\beta} a_{\alpha,\beta}\delta_{\alpha,0}\delta_{\beta,0} U_1^\alpha U_2^\beta = a_{00} I = \frac{tr(\rho)}{2^n} I = \frac{I}{2^n}.$$

So, it is a quantum perfect encryption.□

Similarly, it's easy to prove that $\{p_k = \frac{1}{2^{2n}}, U_k = Y^\alpha H^\beta, k = (\alpha,\beta), \alpha,\beta \in \{0,1\}^n\}$ also forms a PQC. So $\sum\limits_m \alpha_m |m\rangle_I\langle m|$ is an ultimately mixed state.

Thus, the message state σ_1 for the adversary is:

$$\begin{aligned}\sigma_1 &= \sum_m \alpha_m |m\rangle_I\langle m| \otimes \sum_{s,r,r_A} |F_s(m)\oplus r\|r_A\rangle_{II}\langle F_s(m)\oplus r\|r_A| \\ &= \frac{I}{2^n} \otimes \frac{I}{2^n} \\ &= \frac{I}{2^{2n}}. \qquad (17)\end{aligned}$$

Since σ_1 is an ultimately mixed state, the adversary cannot acquire anything by measuring it.

In the second round of communication, the transmitted message state becomes:

$$\sigma_2 \;=\; \sum_{m,s,r_A,r_B} \alpha'_m |m\rangle_I\langle m| \otimes |F_s(m) \oplus r_A \| r_B\rangle_{III}\langle F_s(m) \oplus r_A \| r_B| \quad (18)$$

Supposed that the adversary is able to intercept it, the quantum state for him is also an ultimately mixed state:

$$\sigma_2 \;=\; \frac{I}{2^{2n}}. \quad (19)$$

Similarly, in the third round, the transmitted message state is also an ultimately mixed state:

$$\begin{aligned} \sigma_3 &= \sum_m \alpha''_m |m\rangle_I\langle m| \otimes |F_s(m) \oplus r_B \| r_C\rangle_{IV}\langle F_s(m) \oplus r_B \| r_C| \\ &= \frac{I}{2^{2n}}. \end{aligned} \quad (20)$$

Above analysis shows that the preshard s, r and secret information x will not be disclosed to the attacker. MIM attack is not effective in this protocol. The adversary has no useful method to attack.

Remark 1. There are many special cases satisfying the conditions of U_1 and U_2, such as X and Z, X and Y, Y and H, X and H. Thus, the following examples are all quantum perfect encryptions.

1. PQC1:$\{p_k = \frac{1}{2^{2n}}, U_k = X^\alpha Z^\beta, k = (\alpha, \beta), \alpha, \beta \in \{0,1\}^n\}$.
2. PQC2:$\{p_k = \frac{1}{2^{2n}}, U_k = X^\alpha Y^\beta, k = (\alpha, \beta), \alpha, \beta \in \{0,1\}^n\}$.
3. PQC3:$\{p_k = \frac{1}{2^{2n}}, U_k = X^\alpha H^\beta, k = (\alpha, \beta), \alpha, \beta \in \{0,1\}^n\}$.
4. PQC4:$\{p_k = \frac{1}{2^{2n}}, U_k = Y^\alpha H^\beta, k = (\alpha, \beta), \alpha, \beta \in \{0,1\}^n\}$.

1. When we choose the PQC1: $\{p_k = \frac{1}{2^{2n}}, U_k = X^\alpha Z^\beta, \alpha, \beta \in \{0,1\}^n\}$ for QNK protocol, it is insecure to transmit classical information. Because X operation is to reverse the bit and the function of Z operation is to shift the phase. Thus the attacker can measure the ciphertext state in the basis $\{|0\rangle, |1\rangle\}$ without breaking it. And because the three ciphertext transmitted between Alice and Bob are

$X^{\alpha_A}Z^{\beta_A}|m\rangle$, $X^{\alpha_B}Z^{\beta_B}X^{\alpha_A}Z^{\beta_A}|m\rangle$,$X^{\alpha_B}Z^{\beta_B}|m\rangle$, the attacker can acquire three strings $\alpha_A \oplus m, \alpha_B \oplus \alpha_A \oplus m, \alpha_B \oplus m$ by measuring the three ciphertext. The attacker can computes α_B with the first string and the second string. Then he can computes the message m with the value of α_B and the third string.

2. When choosing the PQC2: $\{p_k = \frac{1}{2^{2n}}, U_k = X^{\alpha}Y^{\beta}, \alpha, \beta \in \{0,1\}^n\}$ for the quantum no-key protocol, it is also unsafe to transmit classical information for the same reason. In this case, the three ciphers transmitted between Alice and Bob is $X^{\alpha_A}Y^{\beta_A}|m\rangle$,$X^{\alpha_B}Y^{\beta_B}X^{\alpha_A}Y^{\beta_A}|m\rangle$, $X^{\alpha_B}Y^{\beta_B}|m\rangle$, measuring the three ciphers can achieve the three strings $\alpha_A \oplus \beta_A \oplus m, \alpha_B \oplus \beta_B \oplus \alpha_A \oplus \beta_A \oplus m, \alpha_B \oplus \beta_B \oplus m$. The attacker can computes $\alpha_B \oplus \beta_B$ with the first string and the second string. Then he can computes the message m with the value of $\alpha_B \oplus \beta_B$ and the third string.

3. In PQC3:$\{p_k = \frac{1}{2^{2n}}, U_k = X^{\alpha}H^{\beta}, k = (\alpha, \beta), \alpha, \beta \in \{0,1\}^n\}$, X and Y do not satisfy the condition that X and Y should form an orthonormal basis.

4. By using $Y^{\alpha}H^{\beta}$ in the protocol, the message is being encoded into the conjugate coding, and the flaw stated in the above disappears. If using POC1 and POC2, after the classical bits being encoded into computational basis state, it will stay in computational basis state during the exchange in the protocol. It is better to choose the PQC4: $\{p_k = \frac{1}{2^{2n}}, U_k = Y^{\alpha}H^{\beta}, k = (\alpha, \beta), \alpha, \beta \in \{0,1\}^n\}$ for the quantum no-key protocol.

Next, we take another attack into account. Assume that the adversary intercepts all the transmitted ciphertext during one session between Alice and Bob. The transmitted ciphertext during the three rounds of communication are:

$$\begin{aligned}
\sigma_1 &= \sum_{m,s,r,r_A} \alpha_m |m\rangle_I\langle m| \otimes |F_s(m) \oplus r\|r_A\rangle_{II}\langle F_s(m) \oplus r\|r_A|, \\
\sigma_2 &= \sum_{m,s,r_A,r_B} \alpha_m^{'} |m\rangle_I\langle m| \otimes |F_s(m) \oplus r_A\|r_B\rangle_{III}\langle F_s(m) \oplus r_A\|r_B|, \\
\sigma_3 &= \sum_{m} \alpha_m^{''} |m\rangle_I\langle m| \otimes |F_s(m) \oplus r_B\|r_C\rangle_{IV}\langle F_s(m) \oplus r_B\|r_C|.
\end{aligned}$$

The whole quantum state from adversary's viewpoint is:

$$\begin{aligned}
&\sum_{m_1,m_2,m_3}\sum_{s,r,r_A,r_B,,r_C}\alpha_{m_1}\alpha^{'}_{m_2}\alpha^{''}_{m_3}|m_1,m_2,m_3\rangle_I\langle m_1,m_2,m_3| \\
&\otimes|F_s(m_1)\oplus r\|r_AF_s(m_2)\oplus r_A\|r_B,F_s(m_3)\oplus r_B\|r_C\rangle_{II}\times \\
&\quad\times_{II}\langle F_s(m_1)\oplus r\|r_A,F_s(m_2)\oplus r_A\|r_B,F_s(m_3)\oplus r_B\|r_C|. \qquad (21)
\end{aligned}$$

In [9] , the conclusion is that the authentication key cannot be used forever in the QNK protocol with 3 rounds or less than 3 rounds of communication. If we consider the trace distance between the direct product of any two ciphertext among the three transmitted ciphertext in the proposed QNK protocol in Section 2, we cannot have the result that such trace distance is zero for different plaintext and authentication keys s, r. As a result, we cannot prove the permanent use of authentication keys s, r. Guaranteed by the no-cloning theorem, the adversary is unable to copy the unknown quantum state transmitted in the channel. The participants involved in the communication process send message with identification. The message without identity information is not send out into the channel. All the three ciphertext cannot be possessed by the adversary at the same time. So, the coefficients $\alpha_{m_1},\alpha^{'}_{m_2},\alpha^{''}_{m_3}$ are distributed in different time and space. The product of $\alpha_{m_1},\alpha^{'}_{m_2},\alpha^{''}_{m_3}$ is zero. Thus, it's no use in computing the trace distance between the direct product of any two ciphertext among the three transmitted ciphertext. Moreover, it's also no used in demonstrating that the quantum state show in formula 21 is an ultimately mixed state.

4. Discussion

QNK protocol cannot resist MIM attack without identification. The QNK protocol based on PQC without identification is as bellow:

1. Alice encrypts ρ with $Y^{\alpha_A}H^{\beta_A}$, and sends Bob $\rho_1 = Y^{\alpha_A}H^{\beta_A}\rho H^{\beta_A}Y^{\alpha_A}$.

2. Bob encrypts ρ_1 with $Y^{\alpha_B}H^{\beta_B}$ and sends Alice $\rho_2 = Y^{\alpha_B}H^{\beta_B}\rho_1 H^{\beta_B}Y^{\alpha_B}$.

3. Alice decrypts ρ_2 with $H^{\beta_A}Y^{\alpha_A}$ and sends Bob $\rho_3 = H^{\beta_A}Y^{\alpha_A}\rho_2 Y^{\alpha_A}H^{\beta_A}$.

4. Bob decrypts ρ_3 with $H^{\beta_B}Y^{\alpha_B}$ to recover ρ.

If attacker Eve intercepts the message ρ_1 from Alice, he randomly selects bit strings α_E and β_E to encrypt ρ_1 and sends Alice $\rho_2^{'} = Y^{\alpha_E} H^{\beta_E} \rho_1 H^{\beta_E} Y^{\alpha_E}$. Alices decrypts $\rho_2^{'}$ with $H^{\beta_A} Y^{\alpha_A}$ and sends Eve $\rho_3^{'} = H^{\beta_A} Y^{\alpha_A} \rho_2^{'} Y^{\alpha_A} H^{\beta_A}$. Eve receives $\rho_3^{'}$ and decrypts it with $H^{\beta_E} Y^{\alpha_E}$. Finally, Eve can get message ρ successfully.

In section 2, we add identification into the protocol to resist MIM attack. Preshard information r and s are necessary in identifying the communicators, so the privacy of r and s are important. We use local random string r_A, r_B, Boolean permutation $F_s(\cdot)$ and quantum entanglement to protect the Alice and Bob's preshared bit strings r and s.

Since the plaintext is encrypted by quantum perfect encyrtion transfromation, the ciphertext state is an ultimately mixed which has nothing to do with the plaintext. In the protocol descryption, we take classical message as example. Moreover, the QNK protocol with identificaiton can be used to transmit quantum message.

5. Conclusions

Quantum no-key encryption protocols are presented based on quantum perfect encryption. We make use of random bit strings, Boolean permutation and the property of entanglement to ensure protocols' security. This protocol with identification can resist MIM attack. The security analysis shows that the pieces of ciphertext of the three rounds are all ultimately mixed states, and the authentication keys can be reused permanently.

Acknowledgement

This work was supported by the National Natural Science Foundation of China under Grant No.61173157.

References

[1] G. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, Crc Press, Boca Raton, 1997.

[2] L. Yang and L. A. Wu, Transmit Classical and Quantum Information Secretly, arXiv: quant-ph/0203089.

[3] L. Yang, L. A. Wu and S. H. Liu, Proc. SPIE, 4917: 106-111, 2002.

[4] Y. Kanamori, S. M. Yoo and A. S. Mohammad, A Quantum No-key Protocol for Secure Data Communication, Proc 43rd ACM SE Conference, ACM Press, New York, 2005.

[5] S. Kak, A Three Stage Quantum Cryptography Protocol, Foundations of Physics Letters **19**(3), 2006.

[6] W. H. Kye, C. M. Kim, M. S. Kim and Y. J. Park, Quantum Key Distribution with Blind Polarization Bases, *Phys. Rev. Lett*, **95**(4): 040501, 2005.

[7] L. Yang, Quantum no-key protocol for direct and secure transmission of quantum and classical messages, arXiv preprint quant-ph/0309200.

[8] Y. Wu and L. Yang, Practical quantum no-key protocol with identification, IAS 2009: 540-543, IEEE Computer Society, 2009.

[9] L. Yang, Quantum no-key protocol for secure communication of classical message, arXiv:1306.3388, 2013.

[10] P. Boykin and V. Roychowdhury, Optimal Encryption of Quantum Bits, *Phys. Rev. A*, **67**, 042317, 2003.

[11] A. Ambainis et al, Private quantum channels,41st Annual Symposium on Foundations of Computer Science, Proceedings:547-553, 2000.

[12] A. Nayak and P. Sen, Invertible quantum operations and perfect encryption of quantum states, *QUANTUM INF COMPUT*, **7**(1-2):103-110, 2007.